IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 20, 2019, accepted April 30, 2019, date of publication May 2, 2019, date of current version May 17, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2914454

An Efficient Web Authentication Mechanism Preventing Man-In-The-Middle Attacks in Industry 4.0 Supply Chain

ALIREZA ESFAHANI[1], GEORGIOS MANTAS[1], JOSÉ RIBEIRO[1], JOAQUIM BASTOS[1], SHAHID MUMTAZ[1], MANUEL A. VIOLAS[2], A. MANUEL DE OLIVEIRA DUARTE[2], AND JONATHAN RODRIGUEZ[2,3]

[1]Instituto de Telecomunicações (IT), P-3810-193 Aveiro, Portugal
[2]Universidade de Aveiro, Aveiro, Portugal
[3]University of South Wales, Pontypridd CF37 1DL, U.K.

Corresponding author: Alireza Esfahani (alireza@ av.it.pt)

This work was supported in part by the Power Semiconductor and Electronics Manufacturing 4.0 (SemI40) Project, under Grant 692466, in part by the Fundação para a Ciência e Tecnologia, under Grant ECSEL/0009/2015, from Austria, Germany, Italy, France, and Portugal, and in part by the Electronic Component Systems for European Leadership Joint Undertaking (ECSEL JU).

ABSTRACT The fourth industrial revolution (Industry 4.0) is transforming the next generation of the supply chain by making it more agile and efficient compared with the traditional supply chain. However, data communication across the partners in the Industry 4.0 supply chain can be the target of a wide spectrum of attackers exploiting security breaches in the internal/external environment of the partners due to its heterogeneous and dynamic nature as well as the fact that the non-professional users in security issues usually operate their information systems. Attackers can compromise the data communication between legitimate parties in the Industry 4.0 Supply Chain, and thus, jeopardizing the delivery of services across the partners as well as the continuity of the service provision. Consequently, secure data communications across the partners in the Industry 4.0 Supply Chain are of utmost importance. Toward this direction, TLS protocol, which is the de facto standard for secure Internet communications, is employed to ensure secure communication between a user's web browser and a remote web server located in the premises of the same or another partner. However, over the last few years, there have been several serious attacks on TLS, including man-in-the-middle attacks in web applications using TLS to secure HTTP communication. Therefore, in this paper, we propose an efficient TLS-based authentication mechanism, which is resistant against MITM in web applications.

INDEX TERMS TLS, MITM attack, authentication, impersonation, HTTPS, Industry 4.0 Supply Chain.

I. INTRODUCTION

Over the past few years, we have witnessed the emergence of the fourth Industrial Revolution (Industry 4.0), where man, machine, and product will be interconnected throughout the whole Supply Chain from the production floor to the managerial level [1]–[10]. However, the emergence of Industry 4.0 will also affect the next generation of the Supply Chain by transforming it to a more agile and efficient compared to the traditional Supply Chain. This will boost the productivity and allow customized and flexible production while benefiting from the economies of scale [11], [12]. Nevertheless, despite the benefits that Industry 4.0 will bring in the Supply Chain, the high degree of interconnectivity among the partners in the Industry 4.0 Supply Chain raises many security challenges that should be addressed effectively and efficiently before the next generation of the Supply Chain reaches its full potential in Industry 4.0 era [1], [2], [13]–[16].

In fact, data communication across the partners in the Industry 4.0 Supply Chain can become a soft target of many known and unknown security threats exploiting security breaches in the internal/external environment of the partners due to its heterogeneous and dynamic nature as well as the fact that employees without cybersecurity awareness usually operate the information systems [2]. Particularly, these vulnerabilities in the Industry 4.0 Supply Chain can be exploited by attackers with a wide spectrum of motivations ranging from criminal intents aimed at financial gain to industrial espionage and cyber-sabotage. Attackers can compromise the data communication between legitimate parties in the

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran.

Industry 4.0 Supply Chain and thus, can jeopardize the delivery of services across the partners as well as the continuity of the service provision [2], [13]. As a result, Industry 4.0 Supply Chain partners will suffer from damaging repercussions, which can cause significant revenue loss, destroy their brand, and eventually hinder their advancement. Therefore, secure data communications across the partners in the Industry 4.0 Supply Chain are of utmost importance [2]. Towards this direction, TLS protocol, which is the de facto standard for secure Internet communications, is employed to ensure secure communication between a user's web browser and a remote web server located in the premises of the same or another partner. However, over the last few years, there have been several serious attacks on TLS including Man-In-The Middle attacks against web applications that use the TLS protocol to secure HTTP communication [23].

Therefore, in this paper, we propose an efficient TLS-based authentication mechanism which is resistant against MITM attacks in web applications that use the TLS protocol to secure HTTP communication. Specifically, the proposed mechanism prevents the attacker from impersonating the legitimate server to the user (i.e., client), with the objective of impersonating the user to the server and thus comprising user's sensitive information. Our TLS-based authentication mechanism is based on the SISCA mechanism which is proposed in [22] and relies on Channel ID-based authentication and server invariance. Compared to the SISCA mechanism, our proposed authentication mechanism reduces the communication overhead by 50 %, while its computational overhead is almost equal to the computational overhead of the SISCA authentication mechanism.

The rest of this paper is organized as follows. Section II gives an overview of the TLS protocol and the state-of-the-art of countermeasures for TLS MITM attacks. Section III presents the proposed TLS authentication mechanism and Section IV provides the security analysis of the proposed mechanism. Section V includes the analysis of the performance evaluation of the proposed mechanism and Section VI shows details of its implementation on a test-bed. Finally, Section VII concludes the paper.

II. RELATED WORK

In this Section, we give an overview of the TLS protocol and the state-of-the-art the countermeasures for TLS MIMT attacks [6], [24].

A. TLS PROTOCOL

The TLS protocol is used to establish a connection between two parties in a secure way. TLS can be considered as version 3.1 of SSL, as it is based on SSL 3.0 Protocol [25]. The main objective of this protocol is to provide privacy and data integrity between two communicating entities over the Internet. TLS consists of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol is at the lowest level and provides connection security that has two basic properties: a) the connection is private and b) the connection is reliable. To achieve the first property (i.e., private connection), symmetric cryptography is used for data encryption, where the keys are generated uniquely for each connection and are based on a secret, negotiated by the TLS Handshake Protocol. On the other hand, to achieve the second property (i.e., reliable connection), the message transport includes a message integrity check using a keyed MAC [25]. On top of the TLS Record Protocol, the TLS Handshake Protocol runs to allow the two communication entities to authenticate each other and to negotiate a cipher and cryptographic keys before the application protocol transmits/receives its first byte of data. In particular, the TLS Handshake Protocol provides connection security with the following three basic properties. Firstly, the communicating entities can authenticate each other by using asymmetric cryptography (e.g., RSA). Secondly, the negotiation of a shared secret is secure so that the secret will remain unavailable to an attacker (i.e., eavesdropper), and for any authenticated connection the secret cannot be revealed to the attacker; Finally, the negotiation is reliable so that an attacker will not be able to modify the negotiation without being detected by the communicating entities [25].

B. TLS MITM ATTACKS AND COUNTERMEASURES

In MITM attack, first, the adversary positions herself in the network path between the victim's browser and the server. When the victim sends a request for establishing a new TLS connection with the server, the adversary intercepts and responds to it using a forged certificate. If the victim accepts this certificate, then she completes the TLS setup with the adversary, who has, as a result, successfully masqueraded as the server. Simultaneously, the adversary establishes a new TLS connection with the server. At this point, the adversary has two active TLS connections: one with the victim and one with the server. However, from the victim's and server's perspectives, there is only one secure connection in place. The adversary can now decrypt, re-encrypt and forward all the messages exchanged between the victim and the server. As a result, the adversary can access private information (e.g., passwords) or even modify it (e.g., code injection). Most browsers perform multiple checks to validate TLS servers certificates and authenticate the server-side of the communication. If any of these checks fails (e.g., MITM attack), the browser relies on security indicators (e.g., warnings messages) to notify the user. However, most of the users tend to ignore these indicators due to the lack of training and high false positive rates [26]–[28]. Many existing defense mechanism against TLS MITM attacks have been proposed and adopted in real-world systems recently [20], [22], [29]–[34]. These mechanisms are classified into two types. The first type focuses on enhancing the certificate authentication model where prevents an adversary from impersonating the server by using a valid certificate that has been misissued [32]–[34]. The second type focuses on strengthening client authentication. Strong client authentication aims to

TABLE 1. Existing TLS MITM countermeasures.

TLS MITM Countermeasure	Mechanism	Feature	Disadvantage	Related Work
Certificate Enhancement	multiple browser-based mechanisms	keep track of certificates	lack of user training	[17]
	certificate pinning	white-list of certificates	neither flexible nor scalable	[18]
	third-parties	certificate is validated by one or more third-parties	operational costs, privacy concerns, and more complex revocation procedures	[19]
Strengthening Client Authentication	Channel ID	self-signed certificate is generated	still vulnerable to MIMT	[20]–[22]

prevent an adversary to steal the user credential information even if she can successfully impersonate the server to the user.

In order to enhance the certificates, one approach is multiple browser-based mechanisms where browser extensions can keep track of the certificates used by the browser and can detect certificate changes [17]. However, the effectiveness of this approach is affected by false positives and lack of user training. Another approach, known as certificate pinning [18], uses a white-list of certificates for important domains in order to reduce the incidence of MITM attacks due to compromised certification authorities and other authentication errors and attacks. This solution is less prone to false positives; however, it is neither flexible nor scalable. Furthermore, the most popular approach is the use of additional third-parties to extend or replace the rigid CA trust model. In this approach, users can select one or more third-parties to confirm the authenticity of a certificate in order to improve the chances of detecting a MITM attack [19]. However, this approach has several shortcomings such as significant deployment and operational costs (e.g., additional infrastructure with high availability requirements), more complex trust model for users, privacy concerns and more complex revocation procedures. Therefore, the inherent complexity and costs associated with third-party solutions have prevented their widespread deployment. As a result, most users still rely on weak certificate validation checks to detect MITM attacks.

Strong client authentication prevents user credential theft or renders it useless, even if the attacker can successfully impersonate the server to the user. One prominent proposal on strong client authentication is the channel ID mechanism which proposed by Balfanz and Hamilton in [20]. The channel ID mechanism is a TLS extension and originally was proposed as Origin-Bound Certificates (OBCs) [21]. Channel ID enables browsers to generate self-signed certificate to conduct TLS client-side authentication, and further prevent MITM attackers to impersonate as the victim's browsers. Google Chrome uses this mechanism and it is expected that the channel ID to be used in the second factor authentication standard U2F, proposed by the FIDO alliance [35]. The U2F is designed to provide strong authentication for users on the web while preserving the user's privacy. The user carries a 'U2F device' as a second factor. However, the U2F device protocol can only detect the most situations in the MITM attack, and not all the situations.

However, Karapanos and Capkun showed that Channel ID-based approaches are still vulnerable to TLS MIMT attack [22]. In this regards, they have proposed the SISCA authentication mechanism which combines Channel ID-based approach with the server invariance. Server invariance is based on sender invariance which was formally defined in [36]. The summary of related work is described in Table 1.

III. THE PROPOSED TLS-BASED AUTHENTICATION MECHANISM

A. ADVERSARY MODEL AND GOALS

The TLS protocol enables users to access their online accounts securely. Moreover, the user authentication credential information is protected by TLS. However, it is necessary to verify the server's authenticity during the TLS connection establishment. If the adversary impersonates the legitimate server to the user (i.e., client), then it can impersonate the user to the legitimate server in order to steal the user's credential information and use them for further malicious activities (e.g., compromise communication, transactions). This attack is known as TLS Man-In-The-Middle (MITM) [22], [23] (see Figure 1).

B. THE PROPOSED MECHANISM

We assume that prior to the mechanism execution, the TLS protocol is established between the client (Partner A) and the server (Partner B) in Industry 4.0 Supply Chain. Then, the server generates one key K_s which is used for all mechanism executions (i.e., not for a specific client) and is never disclosed to other parties. It is important to note that the messages are exchanged within the first HTTP request/response pair. Moreover, we have considered that the server and client deploy Channel ID-based authentication. Thus, each TLS connection will therefore have a channel ID Cid_b that is created by the user's browser and is also known by the server. The proposed mechanism consists of two phases:

- **Initialization:**
  The purpose of this phase is to make a preparation for the client authentication. In our proposed mechanism, once the browser establishes a TLS connection (for the

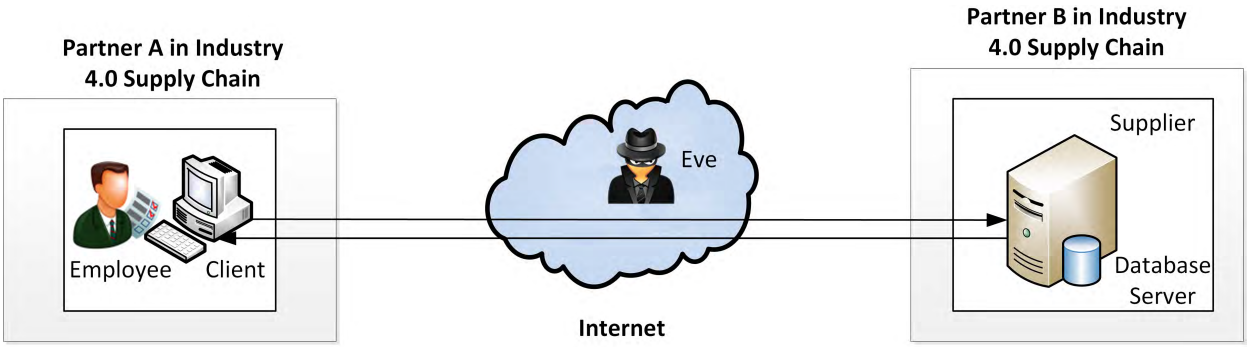


FIGURE 1. The man-in-the-middle attack scenario in Industry 4.0 Supply Chain.

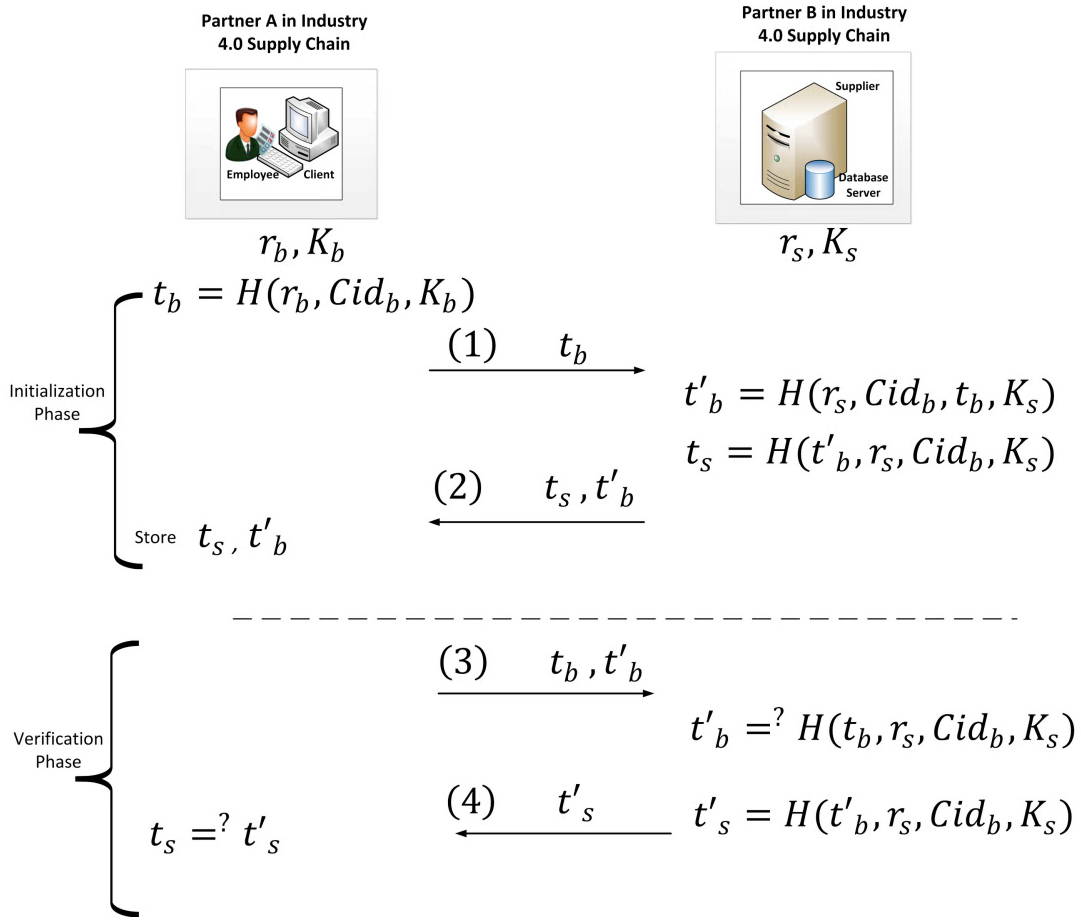


FIGURE 2. The proposed TLS-based authentication mechanism.

first time in a browsing session), the initialization phase occurs. First, the browser uses a pseudorandom number generator (PRNG) to generate randomly the number r_b and the key K_b. Then, the browser calculates the secret value of t_b as follows:

$$t_b = H(r_b, K_b, Cid_b) \tag{1}$$

where Cid_b is the browser's channel ID and $H(.)$ is a collision resistance hash function (i.e., SHA-1). Afterwards, the browser sends t_b within the first HTTP request to the server (step 1), as it is shown in Figure 2. The server calculates two security parameters t'_b and t_s based on the following equations:

$$t'_b = H(r_s, Cid_b, t_b, K_s) \tag{2}$$

$$t_s = H(t'_b, r_s, Cid_b, K_s) \tag{3}$$

These parameters are used on the server side in order to check the originality of t_b and t'_b, respectively. K_s and r_s are the server's key and a random number which

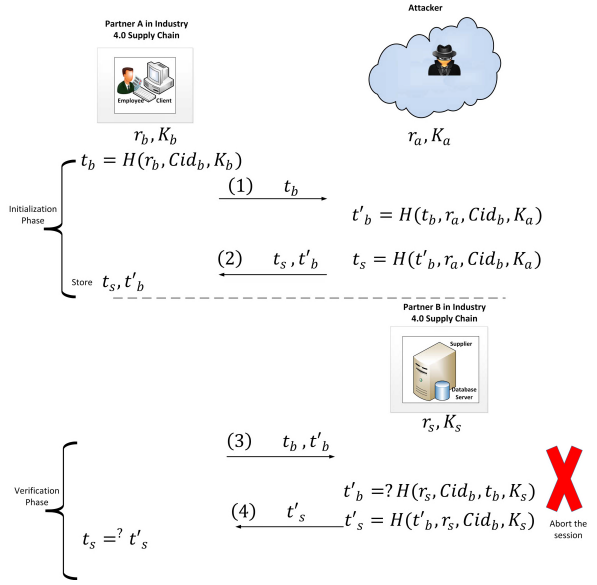


FIGURE 3. Impersonate the initialization phase.

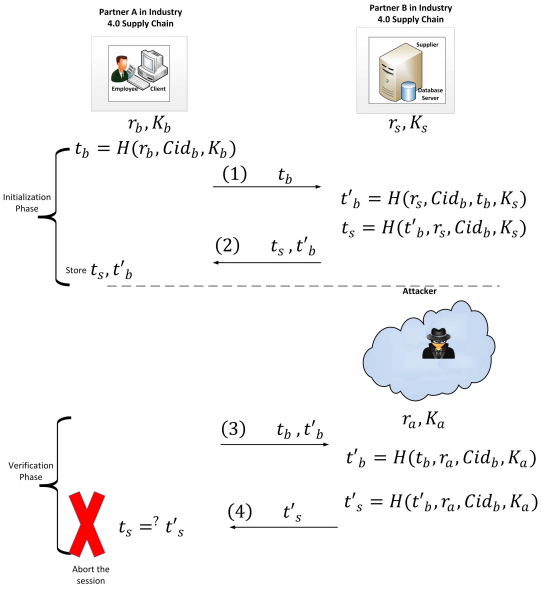


FIGURE 4. Impersonate the verification phase.

is selected randomly by the server, respectively. Next, the server sends back t_s and t'_b within its first HTTP response to the browser (step 2). Finally, the browser stores t_s and t'_b for further communication.

- **Verification:**
The verification phase takes place upon every subsequent TLS connection to the server (Partner B), which occurs within the same browsing session. The browser first sends t_b and t'_b to the server (step 3). Then, the server checks if:

$$t'_b = H(r_s, Cid_b, t_b, K_s) \tag{4}$$

If the check passes, the server calculates t'_s as follows:

$$t'_s = H(t'_b, r_s, Cid_b, K_s) \tag{5}$$

Then, t'_s is sent to the browser (step 4), as it is shown in Figure 2. If t_s (i.e., stored value at the initialization phase) and t'_s are equal on the browser side, then the browser considers that the response arrives from a legitimate server; otherwise, the browser aborts the session.

IV. SECURITY ANALYSIS

In this section, we have provided the security analysis of the proposed mechanism. The security analysis includes two possible attack scenarios. In Figure 3, we illustrate the first attack scenario where the adversary intercepts the initialization phase. In this regard, the adversary needs to inform the browser that has reached the legitimate server. However, the adversary does not have the K_s and Cid_b, because the K_s and Cid_b are securely stored in the server and browser, respectively. Therefore, the adversary will calculate and send to the browser incorrect values of t'_b (i.e., t'_a) and t_s. Thus, the legitimate server recognizes these incorrect values in the verification phase and does not process the request.

The second attack scenario is shown in Figure 4 where the adversary intercepts during the verification phase. In this scenario, however, the adversary receives the t_b and t'_b from the browser, but the adversary does not know the correct value of K_s and Cid_b. Therefore, the adversary calculates and sends to the browser an incorrect value of t'_s which is not equal to the value of t_s that was calculated by the server and stored by the browser in the initialization phase and thus, the browser recognizes these incorrect values in the verification phase and rejects the response.

V. PERFORMANCE EVALUATION

In this section, we compare our proposed mechanism with the SISCA mechanism in terms of communication overhead and computational overhead.

A. COMMUNICATION OVERHEAD

In order to analyze the communication overhead, we assume the overhead of TLS request made by the browser and the TLS response made by the server are negligible. Table 2 is the setting of parameters, based on [37], for calculating the communication overhead of the SISCA authentication mechanism and our proposed authentication mechanism.

TABLE 2. Setting of parameters [37].

Parameters	Description	Value (bits)
t	Hash value/MAC	64
r	random number	128
k	random key	128

The communication overhead of the SISCA mechanism is calculated as follows:

$$C_{SISCA} = \sum_{i=1}^{4} \mid Message_i \mid = 768 \quad bits, \tag{6}$$

TABLE 3. Number of operations required during the initialization and verification phases.

Operations		Initialization		Verification	
		SISCA	Our Mechanism	SISCA	Our Mechanism
random generation	Browser	1	1	0	0
	Server	1	1	0	0
key generation	Browser	0	1	0	0
	Server	2	1	0	0
collision-resistance hash function/MAC	Browser	0	1	0	0
	Server	2	2	2	2

TABLE 4. Time required by initialization and verification phases.

participant	Mechanism	Time consumed
Web browser	SISCA	$2T_H + 2T_r + 2T_k$
	Our mechanism	$3T_H + 2T_r + 2T_k$
Server	SISCA	$2T_H$
	Our mechanism	$2T_H$

where

- $Message_1 =\mid r_b \mid = 128 \quad bits$
- $Message_2 =\mid r_s \mid + \mid t_1 \mid + \mid t_2 \mid = 256 \quad bits$
- $Message_3 =\mid r_b \mid + \mid r_s \mid + \mid t_1 \mid = 320 \quad bits$
- $Message_4 =\mid t_2' \mid = 64 \quad bits$

However, the communication overhead of our proposed mechanism is calculated as follows:

$$C_{proposed-mechanism} = \sum_{i=1}^{4} \mid Message_i \mid = 384 \quad bits, \quad (7)$$

where

- $Message_1 =\mid t_b \mid = 64 \quad bits$
- $Message_2 =\mid t_s \mid + \mid t_b' \mid = 128 \quad bits$
- $Message_3 =\mid t_b \mid + \mid t_b' \mid = 128 \quad bits$
- $Message_4 =\mid t_s' \mid = 64 \quad bits$

According to the above calculation, our proposed authentication mechanism reduces the communication overhead by 50 % compared to the SISCA authentication mechanism.

B. COMPUTATIONAL OVERHEAD

Our proposed authentication mechanism includes the same type of operations (i.e., random generation, key generation, and collision-resistance hash function/MAC) as the SISCA authentication mechanism. Table 3 shows the number of operations required by the browser and the server during the initialization and verification phases of the SISCA authentication mechanism and our proposed authentication mechanism.

We assume that T_H is the computational time required for a collision-resistant hash function, T_r is the time required to generate a random number, and T_k is the time required to generate a random key. Table 4 shows the computational times required by the web browser and server to perform the initialization and verification phases in the SISCA mechanism and our proposed mechanism. As we can see from Table 4, the time required by the web browser and the server to perform the initialization and verification in the SISCA mechanism is approximately $4T_H + 2T_r + 2T_k$, while it is approximately $5T_H + 2T_r + 2T_k$ for our proposed mechanism.

VI. IMPLEMENTATION

The demonstrator is an implementation on a JBoss AS 5.1 server and is optimized for the Microsoft Edge and Google Chrome browsers. The server address is https://id4185:8443/Retailer1 and when the user enters the address into the web browser for the first time, it opens the initialization page. In the initialization page, we can consider three possible scenarios: a) communication between a legitimate browser and a reliable server without considering any MITM attacker, b) communication between a legitimate browser and a reliable server where a MITM attacker is considered between the browser and server during the initialization phase, and c) communication between a legitimate browser and a reliable server where a MITM attacker is considered between the browser and server during the verification phase.

A. SCENARIO A

In the first scenario, the browser has already been registered during the initialization phase and thus it is recognized by the server. As it shown in Figure 5 the browser sends the parameter t_b = 906A46D01100483DA3F2432A537895A92 A8A575 5 and t_b' = B02170FBD00C993FE114CA41E37DF 69EA8CE 89F0 to the server, as these parameters are calculated in the initialization phase. Afterwards, the server responses back to the browser by sending the parameter t_s = 281CB53474E4A7158E78E22E7A44EC9942F7DDEE as it is shown in Figure 6. Then, the browser receives the response and checks if the received parameter t_s' is equal to t_s. If t_s' is equal to t_s, then the browser starts communicating with the server.

B. SCENARIO B

In the second scenario, during the transmission of message 3, as it is shown in Figure 4, the server receives an invalid value of t_b' (e.g., t_b'=196EAA46D4D8D5EE1C149B05A2D915C1 88205C3D, as it is shown in Figure 7). Since this value is calculated and sent by the attacker, the server detects an error and aborts the session.

C. SCENARIO C

In the third scenario, during the transmission of message 4, as it is shown in Figure 5, the browser receives an invalid

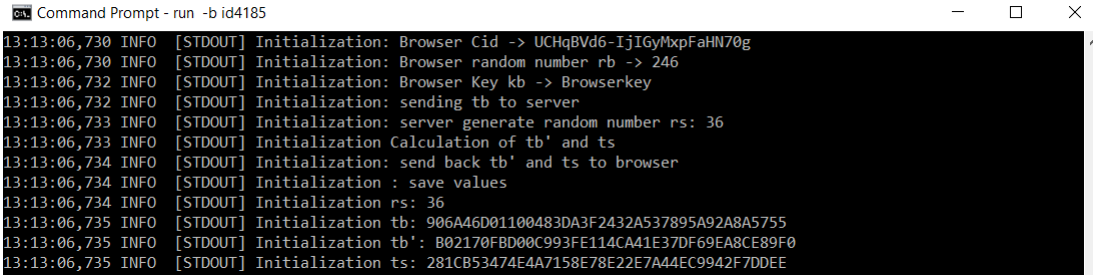


FIGURE 5. The messages exchanged during the initialization phase of our proposed mechanism.

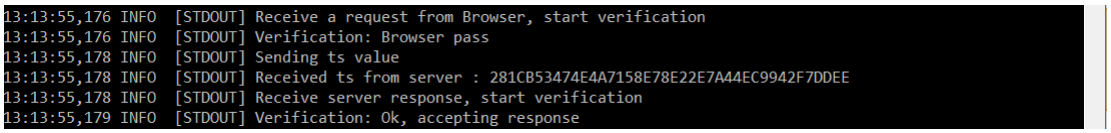


FIGURE 6. Browser's request is accepted.

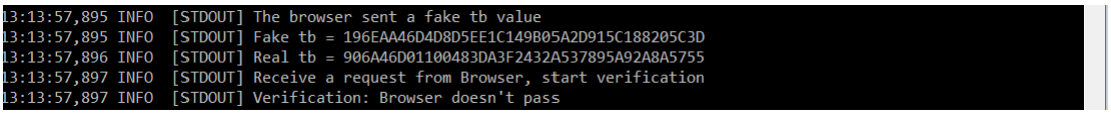


FIGURE 7. Communication between a legitimate browser and a reliable server where a MITM attacker is considered between the browser and server during the initialization phase.

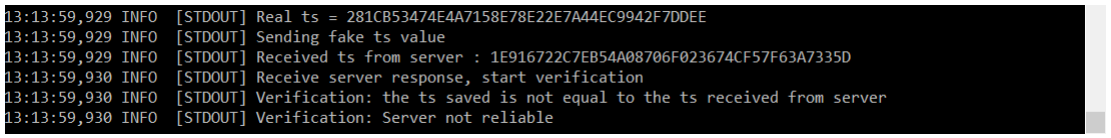


FIGURE 8. Communication between a legitimate browser and a reliable server where a MITM attacker is considered between the browser and server during the verification phase.

value of t_s' (e.g., t_s' = 1E916722C7EB54A08706F023674CF 57F63A7335D, as it is shown in Figure 8). As this value is already calculated and sent by the attacker, the browser detects an error and aborts the session.

VII. CONCLUSION

In this paper, we have proposed an efficient TLS-based authentication mechanism for web applications that use the TLS protocol to secure HTTP communication. Our proposed authentication mechanism prevents the attacker from impersonating the legitimate server to the user (i.e., client), with the objective of impersonating the user to the server and thus comprising user's sensitive information. Our TLS-based authentication mechanism is based on the SISCA mechanism which is proposed in [22] and relies on Channel ID-based authentication and server invariance. Thus, we achieve browser's and server's identity confidentiality and resistance against MITM attacks. Compared to the SISCA mechanism, our proposed authentication mechanism reduces the communication overhead by 50 %, while its computational overhead is almost equal to the computational overhead of the SISCA authentication mechanism. As future work, we plan to implement our proposed mechanism between a client (Partner A) and a server (Partner B) running on two different machines (i.e., two laptops) interconnected over Internet. In addition, we aim to adopt the proposed authentication mechanism to provide lightweight authentication along with resistance against MITM attacks in communications in Industrial IoT networks.

REFERENCES

[1] A. Esfahani *et al.*, "A lightweight authentication mechanism for M2M communications in industrial IoT environment," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 288–296, Feb. 2019.

[2] A. Esfahani *et al.*, "Security framework for the semiconductor supply chain environment," in *Proc. Int. Conf. Broadband Commun., Netw. Syst.* Cham, Switzerland: Springer, 2018, pp. 159–168.

[3] N. Jazdi, "Cyber physical systems in the context of industry 4.0," in *Proc. IEEE Int. Conf. Automat., Qual. Test., Robot.*, May 2014, pp. 1–4.

[4] A. W. Colombo, S. Karnouskos, O. Kaynak, Y. Shi, and S. Yin, "Industrial cyberphysical systems: A backbone of the fourth industrial revolution," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 6–16, Mar. 2017.

[5] L. Wang, M. Törngren, and M. Onori, "Current status and advancement of cyber-physical systems in manufacturing," *J. Manuf. Syst.*, vol. 37, pp. 517–527, Oct. 2015.

[6] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage. (IEEM)*, Dec. 2014, pp. 697–701.

[7] S. Wang, J. Wan, D. Zhang, D. Li, and C. Zhang, "Towards smart factory for Industry 4.0: A self-organized multi-agent system with big data based feedback and coordination," *Comput. Netw.*, vol. 101, pp. 158–168, Jun. 2016.

[8] F. Chen, P. Deng, J. Wan, D. Zhang, A. V. Vasilakos, and X. Rong, "Data mining for the Internet of Things: Literature review and challenges," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 8, 2015, Art. no. 431047.

[9] X. Li, D. Li, J. Wan, A. V. Vasilakos, C.-F. Lai, and S. Wang, "A review of industrial wireless networks in the context of industry 4.0," *Wireless Netw.*, vol. 23, no. 1, pp. 23–41, Jan. 2017.

[10] R. Iqbal, N. Shah, A. James, and J. Duursma, "ARREST: From work practices to redesign for usability," *Expert Syst. Appl.*, vol. 38, no. 2, pp. 1182–1192, 2011.
[11] M. E. Porter and J. E. Heppelmann, "How smart, connected products are transforming companies," *Harvard Bus. Rev.*, vol. 93, no. 10, pp. 96–114, 2015.
[12] R. Iqbal, F. Doctor, B. More, S. Mahmud, and U. Yousuf, "Big data analytics and computational intelligence for cyber–physical systems: Recent trends and state of the art applications," *Future Gener. Comput. Syst.*, to be published.
[13] F. B. Saghezchi *et al.*, "Machine learning to automate network segregation for enhanced security in industry 4.0," in *Proc. Int. Conf. Broadband Commun., Netw. Syst.* Cham, Switzerland: Springer, 2018, pp. 149–158.
[14] S. R. Chhetri, S. Faezi, N. Rashid, and M. A. Al Faruque, "Manufacturing supply chain and product lifecycle security in the era of industry 4.0," *J. Hardw. Syst. Secur.*, vol. 2, no. 1, pp. 51–68, 2018.
[15] J. Wan, J. Li, M. Imran, D. Li, and F. E-Amin, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Trans. Ind. Informat.*, to be published.
[16] Z. Guan *et al.*, "ECOSECURITY: Tackling challenges related to data exchange and security: An edge-computing-enabled secure and efficient data exchange architecture for the energy Internet," *IEEE Consum. Electron. Mag.*, vol. 8, no. 2, pp. 61–65, Mar. 2019.
[17] C. Soghoian and S. Stamm, "Certified lies: Detecting and defeating government interception attacks against SSL (short paper)," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Berlin, Germany: Springer, 2011, pp. 250–259.
[18] C. Evans and C. Palmer, "Certificate pinning extension for HSTS," Tech. Rep., 2011.
[19] P. Hoffman and J. Schlyter. *Using Secure DNS to Associate Certificates With Domain Names for TLS*. Accessed: 2011. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-dane-protocol
[20] D. Balfanz and R. Hamilton, "Transport layer security (TLS) channel IDs, v01 (IETF Internet-draf," 2013.
[21] M. Dietz, A. Czeskis, D. Balfanz, and D. S. Wallach, "Origin-bound certificates: A fresh approach to strong client authentication for the Web," in *Proc. USENIX Secur. Symp.*, 2012, pp. 317–331.
[22] N. Karapanos and S. Capkun, "On the effective prevention of TLS man-in-the-middle attacks in Web applications," in *23rd USENIX Secur. Symp.*, 2014, pp. 671–686.
[23] L. B. Kish, "Protection against the man-in-the-middle-attack for the kirchhoff-loop-Johnson (-like)-noise cipher and expansion by voltage-based security," *Fluctuation Noise Lett.*, vol. 6, no. 1, pp. L57–L63, 2006.
[24] G. Miragliotta, A. Perego, and A. Tumino, "Internet of Things: Smart present or smart future," in *Proc. 17th Summer School Francesco Turco*, 2012.
[25] T. Dierks and E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.2*, document RFC 5246, 2008.
[26] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, "The emperor's new security indicators," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2007, pp. 51–65.
[27] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, "Crying wolf: An empirical study of SSL warning effectiveness," in *Proc. USENIX Secur. Symp.*, Montreal, QC, Canada, 2009, pp. 399–416.
[28] H. Xia and J. C. Brustoloni, "Hardening Web browsers against man-in-the-middle and eavesdropping attacks," in *Proc. 14th Int. Conf. World Wide Web*, 2005, pp. 489–498.
[29] P. Hoffman and J. Schlyter, *The DNS-Based Authentication Of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA*, document RFC 6698, 2012.
[30] P. Hallam-Baker and R. Stradling, *DNS Certification Authority Authorization (CAA) Resource Record*, document RFC 6844, 2013.
[31] J. Hodges, C. Jackson, and A. Barth, *HTTP Strict Transport Security (HSTS)*, document RFC 6797, 2012.
[32] T. H.-J. Kim, L.-S. Huang, A. Perrig, C. Jackson, and V. Gligor, "Accountable key infrastructure (AKI): A proposal for a public-key validation infrastructure," in *Proc. 22nd Int. Conf. World Wide Web*, 2013, pp. 679–690.
[33] B. Laurie, A. Langley, and E. Kasper, *Certificate Transparency*, document RFC 6962, 2013.
[34] D. Wendlandt, D. G. Andersen, and A. Perrig, "Perspectives: Improving SSH-style host authentication with multi-path probing," in *Proc. USENIX Annu. Tech. Conf.*, vol. 8, 2008, pp. 321–334.
[35] S. Srinivas, D. Balfanz, E. Tiffany, F. Alliance, and A. Czeskis, "Universal 2nd factor (U2F) overview," in *Proc. FIDO Alliance Proposed Standard*, 2015, pp. 1–5.
[36] P. H. Drielsma, S. Mödersheim, L. Viganò, and D. Basin, "Formalizing and analyzing sender invariance," in *Proc. Int. Workshop Formal Aspects Secur. Trust*. Berlin, Germany: Springer, 2006, pp. 80–95.
[37] C. Lai, H. Li, R. Lu, and X. S. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Comput. Netw.*, vol. 57, no. 17, pp. 3492–3510, 2013.

ALIREZA ESFAHANI received the Ph.D. degree in telecommunications through the MAP-Tele Doctoral Program, which is a joint venture of Universidade do Minho, Universidade de Aveiro, and Universidade do Porto, in 2017. He joined the Instituto de Telecomunicações (IT) Aveiro, Universidade de Aveiro, in 2012, as a Researcher, and he has been involved in several research projects such as FP7-CODELANCE, SMARTVISION, and ECSEL-SemI40. He is currently a Postdoctoral Fellow of information technology. His research interests include security and cryptography over wireless communications, end-to-end secure communications, the Internet-of-Things (IoT), the IIoT, 5G networks, Blockchain, and secure network coding.

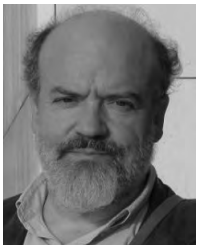
GEORGIOS MANTAS received the Ph.D. degree in electrical and computer engineering from the University of Patras, Greece, in 2012, the M.Sc. degree in information networking from Carnegie Mellon University, Pittsburgh, PA, in 2008, and the Diploma degree in electrical and computer engineering from the University of Patras, Greece, in 2005. He is currently a Senior Researcher with the Instituto de Telecomunicações (IT), Universidade de Aveiro, Aveiro, Portugal, where he is currently involved in research projects such as ECSEL-SemI40, CATRENE-MobiTrust, CATRENE-NewP@ss, ARTEMIS-ACCUS, FP7-CODELANCE, and FP7-SEC-SALUS. His research interests include network and system security, authentication mechanisms, privacy-preserving mechanisms, intrusion detection systems, and secure network coding.

JOSÉ RIBEIRO received the B.Sc. degree (five year course) in telecommunications and electronic engineering and the M.Sc. degree in mobile telecommunications from the Polytechnic Institute of Castelo Branco, Portugal. He is currently pursuing the Ph.D. degree in autonomous and lightweight security for proximity-based applications in smart cities. In 2007, he joined the Instituto de Telecomunicações (IT), Universidade de Aveiro, Aveiro, as a Researcher. He has been involved in European research projects, namely, FP6 ORACLE working on the integration and validation of the project's demonstrator, FP7 HURRICANE working on a platform for vertical handover simulation in heterogeneous networks environments, and FP7 COGEU working on a demonstrator. He was involved in NewP@ss Project promoted by national founding COMPETE, and also had a small participation on the CarCoDe Project as a Reviewer. His main research interests include PHY and MAC advanced techniques, and intrusion detection systems for wireless mobile communications. He has participated in Mobitrust CATRENE Project, reference: CA208. He has some knowledge in programming languages.

JOAQUIM BASTOS received the bachelor's and M.Sc. degrees in electronics and telecommunications engineering from the University of Aveiro, Portugal, in 1997 and 2006, respectively. From 1998 to 1999, he was the Development Manager of Philips, Portugal, where he has participated in National Collaborative Research Projects, and from 1999 to 2002, he had a similar role at Comverse Network Systems, France, in unified communication systems. In 2003, he became a Researcher with the Instituto de Telecomunicações (IT), Universidade de Aveiro, Aveiro, and he has participated in international research projects such as FP6-IST's MATRICE, 4 MORE, and ORACLE, and the WP Leader of FP7-ICT's WHERE and WHERE2, Celtic's MOBILIA, CATRENE's NewP@ss and BENEFIC, and ECSEL's SWARMs. He has authored several conference and journal publications. His main research interests include wireless communication systems, cognitive radio systems, digital signal processing, the IoT, and network security systems and mechanisms.

SHAHID MUMTAZ received the M.Sc. degree in electrical and electronic engineering from the Blekinge Institute of Technology (BTH), Karlskrona, in 2006, and the Ph.D. degree in electrical and electronic engineering from the University of Aveiro, Portugal, in 2011. He has over 10 years of wireless industry experience. He is currently a Senior Research Scientist and the Technical Manager of the Instituto de Telecomunicações (IT), Universidade de Aveiro, Aveiro, Portugal. Prior to his current position, he was a Research Intern with Ericsson and Huawei Research Labs, Karlskrona, Sweden, in 2005. His M.Sc. and Ph.D. degrees were supported by the Swedish Government and FCT Portugal. He has been involved in several EC Research and Development Projects in the field of green communication and next generation wireless systems. In EC projects, he holds the position of Technical Manager, where he oversees the project from a scientific and technical side, managing all details of each work packages, which gives the maximum impact of the projects results for the further development of commercial solutions. He has been also involved in two Portuguese funded projects (SmartVision & Mobilia) in the area of networking, coding, and the development of system level simulator for the 5G wireless systems. He has several years of experience in 3GPP radio systems research with experience in HSPA/LTE/LTE-A and a strong track-record in relevant technology field, especially physical layer technologies, LTE cell planning and optimization, protocol stack, and system architecture. He has over 150 publications in international conferences, journal papers, and book chapters. His research interests include the field of architectural enhancements to 3GPP networks (i.e., LTE-A user plan and control plan protocol stack, NAS, and EPC), 5G NR related technologies, green communications, cognitive radio, cooperative networking, radio resource management, network slicing, LAA/LTU, cross-layer design, Backhaul/Fronthaul, heterogeneous networks, M2M and D2D communication, and baseband digital signal processing.

MANUEL A. VIOLAS received the degree in electronics and telecommunications engineering from the University of Aveiro, Portugal, in 1982, the M.Sc. degree from the University of Coimbra Portugal, 1988, and the Ph.D. degree in electrical engineering from the University of Aveiro, in 1999. Since 1982, he has been with the Department of Electronics and Telecommunications, Universidade de Aveiro, Portugal. From 1990 to 1992, he has conducted research in very broadband optical receivers with British Telecom. He has several publications in conferences and scientific journals, and he has been involved in national and international projects with past projects including OPTRONET, ETOBLU, PHOTON, CELCOP, CROWN, ATLAS, ISIS, FUTON, and BENEFIC. In the scope of the H2020 framework, he was involved in the ECSEL Projects SWARMS (on underwater secure communications) and SEMI40 (on secure communications for Industry 4.0).



A. MANUEL DE OLIVEIRA DUARTE received the M.Sc. degree in telecommunications and the Ph.D. degree in electrical engineering sciences from the University of Essex, U.K., in 1983 and 1984, respectively, and a Licenciatura degree in electrical engineering from the University of Coimbra, Portugal, in 1976. He is currently with the Universidade de Aveiro, Portugal, where he joined, in 1978. In 1988, he has created the Broadband Systems Group, University of Aveiro, over the years, diversified into a series of interrelated research teams, acting in the areas of broadband technologies, optical wireless networks, teletraffic, organization and structure of telecommunications networks and services, and the economic and social aspects of telecommunications. More recently, he became responsible for an educational and Vocational Training Program with the University of Aveiro (Programa Aveiro-Norte), where he was focused in the areas of industrial design, and production technologies and management. Information and communication technologies are widely used in the context of this program as enablers of a learning environment available to a wide variety of users (under and post-graduation students, lifelong students/trainees, and teachers/trainers).

JONATHAN RODRIGUEZ received the master's degree in electronic and electrical engineering and the Ph.D. degree from the University of Surrey, U.K., in 1998 and 2004, respectively. In 2005, he became a Researcher with the Instituto de Telecomunicações (IT), Portugal, where he was a Member of the Wireless Communications Scientific Area. In 2008, he became a Senior Researcher, and he established the 4TELL Research Group targeting next generation mobile systems. He has served as the Project Coordinator of major international research projects, including Eureka LOOP and FP7 C2POWER while serving as the Technical Manager of FP7 COGEU and FP7 SALUS. He is currently the Coordinator of the H2020-SECRET Innovative Training Network. Since 2009, he has been serving as an Invited Assistant Professor with the Universidade de Aveiro, Portugal, and attained Associate Level, in 2015. In 2017, he was an appointed Professor of mobile communications with the University of South Wales, U.K. He has authored over 400 scientific works including 10 book editorials. His professional affiliations include Chartered Engineer (C.Eng.), since 2013, and a Fellow of the IET, in 2015.